Arnold Beckmann
Laurent Bienvenu
Nataša Jonoska (Editors)

Collection of Abstracts

Twelfth Conference on Computability in Europe
CiE 2016: Pursuit of the Universal
Paris, France, June 27 - July 1, 2016

This volume contains abstracts of CiE 2016, including abstracts of invited talks and informal presentations that are not accompanied by publications in the Springer LNCS proceedings of CiE 2016.

Preface

CiE 2016: Pursuit of the Universal
Paris, France, June 27 - July 1, 2016

This year *Computability in Europe* (CiE) honors the 80th anniversary of the A. Turing's paper introducing the Universal Turing Machine. In this context the conference seeks better understanding of universal computational frameworks ranging from mathematics, computer science, through various natural sciences such as physics and biology. CiE provides a forum for exchanging ideas on broad aspects of "computability" striving to understand the essence of computation through studies of theoretical models of new paradigms, information processing, encryption, philosophy and history of computing as well as computability in natural and biological systems. This year's CiE conference meets in Paris and through a sequence of tutorials, plenary lectures and special sessions allows in depth discussions and novel approaches in pursuit of the nature of computability. Similarly to the prior CiE conferences in this series, CiE 2016 has a broad scope promoting the development of computability-related science.

The conference series is organized under auspices of the Association CiE. The association promotes the development of all areas of mathematics, computer science, natural and engineering sciences, that study the notion of "computability", including its philosophical and historical developments. The conference series is a venue where researchers in the field meet and exchange the most novel features of their findings.

CiE 2016 is organized jointly by Université Paris 13 and Université Paris 7, chaired by Paulin de Naurois at Université Paris 13. The previous CiE conferences were held in Amsterdam (The Netherlands) in 2005, Swansea (Wales) in 2006, Siena (Italy) in 2007, Athens (Greece) in 2008, Heidelberg (Germany) in 2009, Ponta Delgada (Portugal) in 2010, Sofia (Bulgaria) in 2011, Cambridge (England) in 2012, Milan (Italy) in 2013, Budapest (Hungary) in 2014, and Bucharest (Romania) in 2015. The proceedings containing the best submitted papers as well as extended abstracts of invited speakers for all these meetings are published in the Springer series *Lecture Notes in Computer Science*.

While computer science conferences usually host formal presentations based on papers published in a proceedings volume, mathematics conferences allow for informal presentations that are prepared very shortly before the conference

and inform the participants about current research and work in progress. So, continuing the tradition of past CiE conferences, CiE 2016 hosts a series of informal presentations, in addition to the presentations based on the papers in the LNCS proceedings volume. This abstract booklet contains, besides short abstracts of some invited talks, abstracts of all informal presentations.

The annual CiE conference has risen to be the largest international meeting focused on computability theoretic issues. CiE 2017 will be held in Turku, Finland. The leadership of the conference series recognizes that there is under representation of female researchers in the field of computability and therefore incorporates a special session *Women in Computability* (WiC) within every CiE conference. WiC initiated in 2007, and was first funded by the *Elsevier Foundation*, afterwards taken over by the publisher *Elsevier*. This year's program, organized by Liesbeth De Mol, besides the regular workshop also provides travel grants for junior female researchers and a mentorship program.

The 39 member program committee of CiE 2016 is chaired by Laurent Bienvenu (IRIF, CNRS & Université Paris 7, France), and Nataša Jonoska (University of South Florida, Tampa, USA). The committee selected the plenary speakers and the special session organizers, and run the reviewing process of all submitted regular contributions.

This year the conference starts with a special session honoring the memory of Barry Cooper, one of the initiators and founders of the conference as well as a driving force behind the organization of CiE, including the presidency of the Association. The session is organized by Mariya Soskova and the contributors are Theodore Slaman (University of California Berkeley), Andrea Sorbi (University of Siena), Dag Norman (University of Oslo) and Ann Copestake (Cambridge University).

Two tutorials are given by Bernard Chazelle from Princeton University, USA and Mikolaj Bojanczyk from University of Warsaw, Poland. In addition, the program committee invited seven speakers to give plenary lectures: Natasha Alechina (University of Nottingham, UK), Vasco Brattka (Universität der Bundeswehr München, Germany), Delaram Kahrobaei (The City University of New York, USA), Steffen Lempp (University of Wisconsin, USA), André Nies (University of Auckland, New Zealand), Dominique Perrin (Université Paris-Est Marne-la-Vallée, France), and Reed Solomon (University of Connecticut, USA).

Springer-Verlag generously funded two awards this year, *Best Student Paper Award* and *Best Paper Award*. The winner of the Best Student Paper Award this year is Mikhail Andreev for his contribution *Busy Beavers and Kolmogorov Complexity*. The Best Paper Award was awarded to Olivier Bournez, Nachum Dershowitz and Pierre Neron for their contribution *An Axiomatization of Analog Algorithms*.

The conference CiE 2016 has six special sessions: two sessions, *Cryptography and information theory* and *Symbolic dynamics*, are organized for the first time in the conference series. The other four special sessions covered new developments in areas previously covered by the conference series: *Computable and constructive analysis*, *Computation in biological systems*, *Weak arithmetic* and *History and*

Philosophy of Computing. Speakers in these special sessions were selected by the special session organizers and were invited to contribute a paper to this volume.

Computable and constructive analysis.
Organizers. Daniel Graça and Elvira Mayordomo.
Speakers. Mathieu Hoyrup (INRIA and University of Lorraine), Arno Pauly (University of Cambridge), Vela Velupillai (New School for Social Research in New York City and University of Trento), Martin Ziegler (KAIST, Daejeon).

Computation in biological systems
Organizers. Alessandra Carbone and Ion Petre.
Speakers. Daniela Besozzi (University of Milan-Biccocca), Eugen Czeizler (Åbo Akademi University), Vincent Moulton (University of East Anglia), Eric Tannier (INRIA and University of Lyon).

Cryptography and information theory.
Organizers. Danilo Gligoroski, and Carles Padro.
Speakers. Ludovic Perret (Université Pierre et Marie Curie, France), Ignacio Cascudo (Aarhus University in Denmark), Oriol Farras (Universitat Rovira i Virgili, Spain), Danilo Gligoroski (Norwegian University of Science and Technology - Trondheim).

History and Philosophy of Computing.
Organizers. Alberto Naibo and Ksenia Tatarchenko
Speakers. Maël Pégny (IHPST, Paris), Pierre Mounier-Khun (CNRS), Simone Martini (University of Bologna), Walter Dean (University of Warwick).

Symbolic dynamics.
Organizers. Jarkko Kari and Reem Yassawi.
Speakers. Valérie Berthé (University Paris 7), Emmanuel Jeandel (University of Lorraine), Irène Marcovici (University of Lorraine), Ronnie Pavlov (Denver University).

Weak arithmetic.
Organizers. Lev Beklemishev and Stanislav Speranski.
Speakers. Pavel Pudlák (Academy of Sciences of the Czech Republic), Alexis Bès (University of Paris 12), Leszek Kołodziejczyk (University of Warsaw), Albert Visser (University of Utrecht).

The organizers of CiE 2016 would like to acknowledge and thank the following entities for their financial support (in alphabetical order): the *Association for Symbolic Logic* (ASL), the *European Association for Theoretical Computer Science* (EATCS), *Springer-Verlag*. We would also like to acknowledge the support of our non-financial sponsor, the *Association Computability in Europe* (CiE).

June 2016

Arnold Beckmann
Laurent Bienvenu
Nataša Jonoska

Organization

Steering Committee

Arnold Beckmann (Swansea, chair), Laurent Bienvenu (Paris), Paola Bonizzoni (Milano), Alessandra Carbone (Paris), Nataša Jonoska (Tampa FL), Benedikt Löwe (Amsterdam & Hamburg), Florin Manea (Kiel), Dag Normann (Oslo), Mariya Soskova (Sofia) and Susan Stepney (York).

Programme Committee

Marcella Anselmo (Univ. of Salerno - DIA)
Nathalie Aubrun (CNRS, INRIA, UCBL, Université de Lyon)
Georgios Barmpalias (Chinese Academy of Sciences)
Marie-Pierre Béal (Université Paris-Est)
Arnold Beckmann (Swansea University)
Laurent Bienvenu (LIAFA, CNRS & Université de Paris 7)
Paola Bonizzoni (Università di Milano-Bicocca)
Alessandra Carbone (Université Pierre et Marie Curie)
Douglas Cenzer (University of Florida)
Liesbeth De-Mol (CNRS, Université de Lille 3)
Volker Diekert (University Stuttgart)
David Doty (California Institute of Technology)
Jérôme Durand-Lose (LIFO - U. D'Orléans)
Martin Escardo (University of Birmingham)
François Fages (Inria Paris-Rocquencourt)
Enrico Formenti (Nice Sophia Antipolis University)
Daniela Genova (University of North Florida)
Noam Greenberg (Victoria University of Wellington)
Hajime Ishihara (JAIST)
Paulin Jacobé De Naurois (CNRS, LIPN, Université Paris 13)
Nataša Jonoska (University of South Florida)
Jarkko Kari (University of Turku)
Lila Kari (University of Western Ontario)
Margarita Korovina (A.P. Ershov Institute of Informatics Systems)
Marta Kwiatkowska (University of Oxford)
Karen Lange (Wellesley College)
Benedikt Löwe (Universiteit van Amsterdam)
Florin Manea (Christian-Albrechts-Universität)
Keng Meng Selwyn Ng (Nanyang Technological University)
Arno Pauly (University of Cambridge)
Mario Perez-Jimenez (University of Sevilla)
Ion Petre (Åbo Akademi University)
Alexis Saurin (PPS & INRIA Pi.R2)
Shinnosuke Seki (University of Electro-Communications, Tokyo)
Paul Shafer (Ghent University)

Alexander Shen (LIRMM CNRS & Univ. Montpellier 2)
Alexandra Soskova (Sofia University)
Mariya Soskova (Sofia University)
Peter van Emde Boas (ILLC-FNWI-Universiteit van Amsterdam)

Additional Reviewers

A
Asher, Nicholas
B
Barash, Mikhail
Bauwens, Bruno
Besson, Tom
Bodirsky, Manuel
C
Calvert, Wesley
Cherubini, Alessandra
Crabbé, Benoit
Cramer, Marcos
Cristescu, Ioana
D
Delacourt, Martin
Dolce, Francesco
E
Ehlers, Thorsten
F
Fokina, Ekaterina
H
Hirschfeldt, Denis
J
Johannsen, Jan
Jolivet, Timo
K
Kach, Asher
Kim, Hwee
Kleinberg, Samantha
Kreuzer, Alexander P.
Kudinov, Oleg
Kuyper, Rutger
M
Manzoni, Luca
Melnikov, Alexander
Michel, Pascal
Minnes, Mia
Monin, Benoît
N
Nemoto, Takako
P
Papazian, Christophe
Paskevich, Andrei
Petre, Luigia
Place, Thomas
Porreca, Antonio E.
R
Raimondi, Franco
Rin, Benjamin
Rizzi, Romeo
Romashchenko, Andrei
S
Salo, Ville
Shafer, Paul
Shlapentokh, Alexandra
Sibelius, Patrick
Sieweck, Philipp
Steiner, Rebecca
Stephan, Frank
Szymanik, Jakub
T
Towsner, Henry
V
van Leeuwen, Jan
Vatev, Stefan
W
Westrick, Linda Brown
Y
Yokoyama, Keita
Z
Zandron, Claudio
Ziegler, Martin

S. Barry Cooper
1943 – 2015

Barry Cooper at the opening of CiE 2009 in Heidelberg.
Photo taken by Peter van Emde Boas, July 2009.

Barry Cooper, founding member and former president of the Association Computability in Europe, died on 26 October 2015, shortly after his 72nd birthday. Born on 9 October 1943, Barry was a leading figure in the UK logic scene all of his academic life, a major figure in computability theory, and in particular degree theory. Most relevant in the context of CiE 2016 is of course that Barry was the driving force of Computability in Europe and without him, our Association would not exist. This text is focused on Barry in relation to the Association Computability in Europe, it is based on a short obituary by Benedikt Löwe and Dag Normann [1] and borrows from it with due permission of the authors.

Barry retired from the office of President of the Association CiE in summer 2015, and had the chance to close the Association AGM in Bucharest in July 2015 with a speech reminiscing about the history of the Association. Barry was very fond of telling the ironic tale how our Association with more than a thousand members grew out of a rejected application for European funding.

In order to discuss the negative feedback of the referees, it had been decided to have a conference in Amsterdam which became the first CiE conference. Barry's vision and guidance pushed us along the way, to further CiE conferences and finally to the formal formation of this Association in 2008. In the years 2007 and 2012, he personally co-chaired the programme committees of the CiE conferences in Siena and Cambridge; the fact that these two events were the two largest

CiE conferences to date is a testament to Barry's infectious enthusiasm and inclusive attitude. Barry also realized the potential of the Turing Centenary and made sure that the 100th birthday of Alan Turing was appropriately celebrated during the *Alan Turing Year*, not just in the United Kingdom, but all across the globe; at Turing's alma mater in Cambridge, Barry was one of the organizers of a six-month Turing-related research programme at the Isaac Newton Institute for Mathematical Sciences culminating on Turing's 100th birthday, the 23rd of June 2012, on the lawn in front of King's College. In the years after the Centenary, Barry renamed the *Alan Turing Year* into *Alan Turing Years*; as the media attention to Alan Turing grew, partly due to the Academy-award winning movie *The Imitation Game*, Barry became one of Alan Turing's spokespeople on Twitter and in opinion pieces for the Guardian.

A comprehensive account of Barry's impact on *Computability in Europe* by Benedikt Löwe [2] has been published in the journal *Computability* of our Association.

Barry had been very influential in shaping our thinking about computability in much broader, interdisciplinary terms, which had been key to the success of the movement *Computability in Europe*. His vision will continue to live in us; his stimulating remarks and kindness will be very much missed.

April 2016

Arnold Beckmann
Laurent Bienvenu
Nataša Jonoska

References

[1] Benedikt Löwe and Dag Normann: *Barry Cooper (1943–2015)*. Obituary published on the website of the Association CiE, 28 October 2015.
[2] Benedikt Löwe: *Barry Cooper (1943–2015): The engine of Computability in Europe*. Computability, vol. 5, no. 1, pp. 3-11, 2016.

Table of Contents

Invited Abstracts

Abstracts of Informal Presentations

Verifying Systems of Resource-Bounded Agents

Natasha Alechina

University of Nottingham
Nottingham, UK
nza@cs.nott.ac.uk

Approaches to the verification of multi-agent systems are typically based on games or transition systems defined in terms of states and actions. However such approaches often ignore a key aspect of multi-agent systems, namely that the agents' actions require (and sometimes produce) resources. We briefly survey previous work on the verification of multi-agent systems that takes resources into account, and outline some key challenges for future work. This is joint work with Brian Logan.

Decidability of fragments of arithmetic

Alexis Bes

Département d'informatique, Faculté des Sciences et Technologie
Université Paris-Est Créteil - Créteil Cedex France
bes@u-pec.fr

The study of decidability of fragments of arithmetic is a classical topic in logic, which was initiated by Tarski, Skolem and Presburger in the 1920s. Two of the most important results in this field are Presburger's proof of the decidability of arithmetic without multiplication, and Matiyasevich-Davis-Robinson-Putnam's proof of the undecidability of the existential theory of arithmetic (which provides a negative solution to Hilbert's tenth problem). In this talk, we survey important results and problems in the field, with a focus on the decidable side. In particular, we discuss methods for proving decidability, connections with open problems in number theory, connections between (expansions of) Presburger arithmetic and automata and combinatorics over words, as well as implementation of decision procedures and complexity issues.

Languages recognised by finite algebras

Mikołaj Bojańczyk

University of Warsaw

Regular languages are typically described using automata or regular expressions. There are two important alternatives: logic (regular languages are exactly those languages that can be described using formulas of monadic second-order logic) and algebra (regular languages are exactly those languages that can be recognised by homomorphisms into finite monoids). In my tutorial, I will talk about these two alternatives and their interplay. I will be especially interested in how both logic and algebra can be extended from finite words to other settings, like various kinds of infinite words, or trees or graphs. I will also try to seek common themes among these other settings, and phrase those themes using the language of monads.

Computability and Analysis, a Historical Approach

Vasco Brattka

Universität der Bundeswehr München, Germany

The history of computability theory and and the history of analysis are surprisingly intertwined since the beginning of the twentieth century. For one, Émile Borel discussed his ideas on computable real number functions in his introduction to measure theory. On the other hand, Alan Turing had computable real numbers in mind when he introduced his now famous machine model. Here we want to focus on a particular aspect of computability and analysis, namely on computability properties of theorems from analysis. This is a topic that emerged already in early work of Turing, Specker and other pioneers of computable analysis and eventually leads us to the very recent project of classifying the computational content of theorems in the Weihrauch lattice.

Collective Behavior Via Network-Based Dynamics

Bernard Chazelle

Princeton University

Living systems are often modeled as dynamical systems that enable the emergence of collective behavior from the distributed application of local rules in dynamic networks. This approach raises two issues: How realistic are the models? Can their analyses go beyond numerical simulation? This talk will focus on the second question and provide a short tutorial on a set of novel analytical techniques that have been applied to opinion dynamics, synchronization, swarming, and social learning. This two-part tutorial will assume no prior knowledge on the subject.

The typical constructible object

Mathieu Hoyrup

LORIA - B248
Villers-lés-Nancy, France
hoyrup@loria.fr

Baire Category is an important concept in mathematical analysis. It provides a way of identifying the properties of typical objects and proving the existence of objects with specified properties avoiding explicit constructions. For instance it has been extensively used to better understand and separate classes of real functions such as analytic and smooth functions. Baire Category proves very useful in computability theory and computable analysis, again to understand the properties of typical objects and to prove existence results. However it cannot be used directly when studying classes of computable or computably enumerable objects: those objects are atypical. Here we show how Baire Category can be adapted to such small classes, and how one can define typical computably enumerable sets or lower semicomputable real numbers for instance.

Algorithmic problems in group theory, their complexity and applications to information security

Delaram Kahrobaei

The City University of New York

In this talk I will survey some of the algorithmic problems in group theory such as word, conjugacy, subgroup membership, and geodesic length problems. I will speak about their computability and complexity results in a few classes of groups including metabelian groups (joint results with Conchita Martinez-Perez (Spain) and Jonathan Gryak (CUNY)) as well as hyperbolic groups (joint work with Indira Chatterji (France) and Ni Lu (CUNY, GC)). I will survey some cryptosystems that have been proposed using these problems such as non-commutative Diffie-Hellman (a.k.a. Ko-Lee) key exchange as well as cryptosystems using subgroup distortion (joint with I. Chatterji and N. Lu). There are other group structures that have been proposed for cryptography; particularly a key exchange using semidirect products of (semi)groups. This part of my talk is a joint work with Vladimir Shpilrain (City College of New York). We particularly propose free-nilpotent p-groups for this scheme.

Two frontier problems in bounded arithmetic

Leszek Aleksander Kołodziejczyk

Institute of Mathematics, University of Warsaw
Warsaw, Poland
lak@mimuw.edu.pl

In the mid-1990s, asking an expert "What are the problems on the frontier of research in bounded arithmetic?" would have plausibly led to an answer along the lines of "There are two such problems: (i) separating the relativized bounded arithmetic hierarchy by sentences of fixed quantifier complexity, and (ii) proving a combinatorial independence result for relativized bounded arithmetic with an additional quantifier for counting mod 2".

Today, the answer could very well be the same! In my talk, I plan to discuss these two frontier problems and explain what we have learned in the last two decades.

On Cototality and the Skip Operator in the Enumeration Degrees

Steffen Lempp

Department of Mathematics, University of Wisconsin, Madison, USA

In the enumeration degrees, we study the notion of cototality (first defined by Pankratov and Solon fifteen years ago (cf. the Pankratov abstract for the 200 Mal'cev meeting as well as Solon's 2005 and 2006 papers), a notion which has recently been shown to be relevant to other fields like ergodic theory and group theory (cf. Jeandel, in preparation): An enumeration degree is called *cototal* if it contains a set A with $A \leq_e \overline{A}$. We present several more examples of naturally occurring cototal sets and separate cototality from a number of related notions, like totality, weak cototality and graph totality.

Closely related to this investigation is the notion of the *skip* operator, which we define by letting $A^\Diamond = \overline{K_A}$ where $K_A = \{e \mid e \in \Phi_e(A)\}$. The skip is a weak version of the *jump* $J_e(A)$; indeed $J_e(A) \equiv_e K_A \oplus \overline{K_A} \equiv_e A \oplus A^\Diamond$, but $A <_e J_e(A)$, whereas in general we only have $A^\Diamond \not\leq_e A$. We will present a skip inversion theorem and a number of results that the skip operator can exhibit some bizarre behavior.

This is joint work with Andrews, Ganchev, Kuyper, J. Miller, A. Soskova and M. Soskova.

The wonderful world of RNA

Vincent Moulton

School of Computing Sciences, University of East Anglia
Norwich, UK
Vincent.Moulton@cmp.uea.ac.uk

Boosted by the incredible advances in DNA sequencing, stunning discoveries are being made into how genes and genomes work, and how this knowledge may be applied to important problems in areas such as health, agriculture and human origins. The sister molecule to DNA, RNA, is often less talked about, but current advances concerning this molecule are just as exciting. For example, recent work has shown how RNA's building blocks may have arisen on early earth, which could have profound consequences on our understanding of the origin of life, and small RNAs have taken center stage in biological systems due their role as key regulators within the cell. RNA molecules are interesting from a computational point of view as they can fold up into tree-like structures which can be efficiently predicted and processed. In this talk, we will review some background concerning the computational biology of RNA, and will discuss some recent results and challenges in this fascinating area of research.

Lowness, randomness, and computable analysis

André Nies

Department of Computer Science, University of Auckland

A *lowness notion* provides a sense in which an oracle set A is close to computable. For instance, being computably dominated (each function computed by A is dominated by a computable function) is a lowness notion; so is that the halting problem relative to A has the least possible Turing complexity. Lowness notions have been studied for at least 50 years. More recently, and perhaps surprisingly, randomness has been applied to investigate lowness notions. For instance, K-triviality of a set of natural numbers (i.e., being far from random in a specific sense) coincides with lowness for Martin-Löf randomness, and many other notions.

Analysis allows us to re-interpret many existing randomness notions originally defined in terms of algorithmic tests. For instance, a real z is computably random iff every nondecreasing computable function is differentiable at z, as shown by Brattka, Miller and Nies.

Concepts from analysis have also entered the interaction between lowness and randomness. The Lebesgue density theorem for effectively closed sets C provides two randomness notions for a set Z of natural numbers which are slightly stronger than Martin-Löf's. (In the strong form the density of any C containing Z needs to be 1 at Z; in the weak form, it is merely positive.) These two notions have been used to obtain a Turing incomplete Martin-Löf-random above all the K-trivials, thereby solving the so-called covering problem.

In current research, concepts inspired by analysis are used to stratify lowness notions. Cost functions describe a dense hierarchy of subideals of the K-trivial Turing degrees. The Gamma-parameter of a Turing degree is a real number measuring its complexity in terms of the asymptotic density of bit sequences.

The talk will be introductory.

12

Computation of topological entropy for $\mathbb{Z}^2$ shifts of finite type

Ronnie Pavlov

Department of Mathematics, University of Denver
Denver CO, USA
rpavlov@du.edu

It has been well-known for some time that the topological entropy of a $\mathbb{Z}^2$ shift of finite type may have no closed form, and in fact may even be noncomputable. For this reason, it's worthwhile to find provable approximation schemes for the topological entropy of such systems. I will describe some hypotheses which imply approximation schemes for entropy, with varying computation times. The best such results typically leverage uniqueness of the measure of maximal entropy for the system, but I will conclude by outlining recent joint work (with Adams, Briceno, and Marcus) which allows for efficient approximation for some systems where the measure of maximal entropy is not unique.

Gröbner Bases Techniques in Quantum-Safe Cryptography

Ludovic Perret

Université Pierre et Marie Curie
Paris, France
Ludovic.Perret@gmail.com

After the publication of Shor's algorithm it became evident the most popular public-key cryptographic systems that rely on the integer factorization problem or on the discrete logarithm problem would be easily solvable using large enough quantum computers (if such quantum computers are ever built). That triggered a vivid interest in the research of cryptographic algorithms (mostly public-key cryptographic systems) that are resistant to quantum computers.

Algebraic cryptanalysis is as a general powerful framework which allow to asses the security of a wide range of cryptographic schemes. The basic principle of such cryptanalysis is to model a cryptographic primitive by a set of algebraic equations. The system of equations is constructed in such a way as to have a correspondence between the solutions of this system, and a secret information of the cryptographic primitive. The key problem in algebraic cryptanalysis is to compute a Gröbner basis of the algebraic equations derived from the cryptographic primitive.

It turns that algebraic cryptanalysis can be used to evaluate the security of most quantum-resistant crypto systems proposed so far. The goal of this talk is to quickly discuss of the current intense activity in quantum-resistant cryptography and to present some algebraic attacks against quantum-resistant schemes.

14

Minimal subshifts, Schützenberger groups and profinite semigroups

Dominique Perrin

Université Paris-Est Marne-la-Vallée, France

Almeida and Costa have shown how one can associate to a minimal subshift X on an alphabet A a $\mathcal{J}$-class J in the free profinite semigroup on A. They have shown that if X is a tree set, the Schützenberger group of J is isomorphic to the free group $F(A)$ on A. We relate their result with results obtained by Berthé, De Felice, Dolce, Leroy, Reutenauer and myself concerning the intersection of the set of factors of S with a subgroup of finite index of $F(A)$.

On sentences provable in fragments of bounded arithmetic

Pavel Pudlak

Mathematical Institute, Czech Academy of Sciences
Prague, Czech Republic
pudlak@math.cas.cz

Bounded arithmetic refers to the system of relatively weak subsystems of Peano Arithmetic that are loosely connected with complexity classes studied in computational complexity. Typically, the induction schema is restricted to a class of formulas that define a particular complexity class and provably total functions (defined by a suitably restricted class of formulas) are functions computable in a particular complexity class.

The basic problem studied in bounded arithmetic is similar to the problems in computational complexity: to prove separations of theories, i.e., to prove that one theory is stronger (or non conservative over a given class of formulas) than another one. As in computational complexity, these problems do not seem to be amenable to current mathematical methods. Nevertheless, by giving combinatorial characterization of sentences provable in the studied theories we can, at least, get some partial evidence for our conjectures about which theories are stronger.

Combinatorial characterization of provable $\forall\Sigma^b_1$ sentences have been obtained for the main first order fragments T^i_2 and two second order fragments U^1_2 and V^1_2. In this lecture we will present an approach which possibly may lead to characterizations of such sentences in the (probably) stronger fragments V^i_2, for $i \geq 2$.

16

Stability in reverse mathematics and computable reductions

Reed Solomon

University of Connecticut, USA

In reverse mathematics, it is often useful to separate combinatorial principles into stable and cohesive versions. We will discuss examples of this phenomena and present recent work on several stable combinatorial principles from the point of view of Weihrauch and computable reducibility. The main results are joint work with Eric Astor, Damir Dzhafarov, Ludovic Patey, Jacob Suggs and Linda Brown Westrick.

On random graphs and the evolution

Eric Tannier

UMR CNRS 5558 Laboratoire de Biométrie et Biologie Évolutivé
INRIA, France
eric.tannier@inria.fr

The 1960 paper of Erdös and Renyi was entitled "On the evolution of random graphs". They mention possible applications in many fields, but not in evolution. I will show such an application. Evolution on genomic sequences will be an accumulation of inversions. I will show that this process is, with a reasonable approximation, similar to the accumulation of edges in a graph, where each vertex i is associated with a probability p_i, and an edge is taken with probability $p_i p_j$. This analogy is helpful to estimate unknown parameters (how many inversions i.e. edges?) from observable ones (how many conserved pairs of consecutive genes i.e. isolated vertices?).

Restricted sequential theories

Albert Visser

Philosophy, Faculty of Humanities, Utrecht University
Utrecht, The Netherlands
a.visser@uu.nl

A theory is *sequential* if it contains a good theory of sequences. Examples of sequential theories are Elementary Arithmetic, Peano Arithmetic, ACA_0, Zermelo-Fraenkel Set Theory and Gödel-Bernays Set Theory. The sequential theories have many good properties. Two classes of sequential theories have been studied with special attention: the finitely axiomatizable ones and the reflexive ones.

In our talk we zoom in on a different class: the restricted theories. A theory is *restricted* if all its axioms have complexity smaller or equal than a given number. The class of restricted sequential theories contains the finitely axiomatized sequential theories. Moreover, some reflexive theories are restricted.

It turns out that the restricted sequential theories share many important properties with the finitely axiomatized ones. For example, every consistent restricted sequential theory has a Σ_1-sound interpretation of the weak arithmetical theory S^1_2.

We will discuss some of these similarities and also some differences. We will give a characterization of interpretability between restricted theories. We discuss the following result. Consider a consistent restricted sequential theory U. For any formula Bx with only x free, we can find a sufficiently small U-definable cut J of a designated class of numbers, such that, if U proves that Bx is witnessed in J, then U proves that Bx has a witness below some standard number.

We draw various consequences from the above result. For example: every consistent, restricted, recursively enumerable sequential theory has a finitely axiomatized extension that is conservative w.r.t. formulas of complexity below n. A special case of this theorem is, for example, that, for every recursively enumerable extension U of Peano Arithmetic, there is a finitely axiomatized extension of ACA_0 with the same arithmetical consequences as U. (This reproves a result of Robert van Wesep of 2013.)

Higher Randomness and hK-Trivials

Anglès d'Auriac Paul-Elliot and Benoît Monin

Université Paris Est-Créteil, Paris, France

Computability gives us tools to define randomness on subsets of natural numbers. We consider a set random if it does not have any typical property, on a given class of properties given by computability theory.

Here, we focus on another notion of computability, which definitions are given by descriptive set theory, but that we can see as computation over ordinal time. These new definitions give rise to similar definitions of randomness, called Higher Randomness.

Some theorems on classical randomness have their counterpart on higher randomness, and some not. The fact that Weak-2-Randoms equals the $\mathrm{ML}\langle 0'\rangle$ does not hold in the higher settings. We show that the sets which fix this fact, by continuous relativizations, are exactly the hK-trivials.

Classifying the computational power of stochastic physical oracles

Edwin Beggs[1], Pedro Cortez[2], José Félix Costa[2,3], and John V. Tucker[1]

[1] College of Science, Swansea University, Singleton Park, Swansea, SA2 8PP, Wales, U.K.
[2] Department of Mathematics, Instituto Superior Técnico, Universidade de Lisboa, Lisboa, Portugal
[3] Centro de Filosofia das Ciências da Universidade de Lisboa, Lisboa, Portugal

Consider an algorithm requesting information from an external source – an *oracle* – the terminology originates with Alan Turing [7]. Emil Post [6] used oracles to study computability.

However, suppose the external source is not a pure mathematical entity but a *physical device or environment*. Suppose the requests are for measurements of physical quantities. We call this external source a *physical oracle*. Algorithms with physical oracles may be found in measurement experiments, and in controlling machines. We ask: *What is the computational power of adding a physical oracle? How does the computational theory depend upon the physical theories and models?*

In [2,3] we developed a computability and complexity theory for physical oracles. The computational classification needed non-uniform complexity classes [1], especially $P/\log\star$ and $BPP//\log\star$ [5]. Using case studies, we formulated axioms expressing properties common to wide classes of physical systems [4].

Here we review physical oracles and report new results broadening their scope by using *non-deterministic physical systems*. Physical oracles with probabilistic theories we call *stochastic physical oracles*. We examine examples of three types of non-deterministic systems, those that that are physically nondeterministic, as in quantum phenomena; physically deterministic but whose physical theory is non-deterministic, as in statistical mechanics; and physically deterministic but whose computational theory is non-deterministic caused by error margins. We prove:

Theorem 1. *Let SPO be the axioms for stochastic physical oracles. Let P be a physical system whose behaviour depends upon a physical quantity or parameter σ. Suppose P satisfies the axioms of SPO. Then: a set $A \subset \{0,1\}^\star$ is decidable in polynomial time by a Turing machine with physical oracle P and unknown parameter σ if, and only if, $A \in BPP//\log\star$.*

References

1. José Luis Balcázar, Josep Días, and Joaquim Gabarró. *Structural Complexity I.* Springer-Verlag, 2nd edition, 1988, 1995.

2. Edwin Beggs, José Félix Costa, Bruno Loff, & John V. Tucker. Computational complexity with experiments as oracles. *Proc. Royal Soc., A (Math., Phys. and Eng. Sci.)*, 464(2098):2777–2801, 2008.
3. Edwin Beggs, José Félix Costa, Bruno Loff, and John V. Tucker. Computational complexity with experiments as oracles II. Upper bounds. *Proc. Royal Soc., Ser. A*, 465(2105):1453–1465, 2009.
4. Edwin J. Beggs, José Félix Costa, and John V. Tucker. Axiomatizing physical experiments as oracles to algorithms. *Phil. Trans. Royal Soc., Ser. A (Math., Phys. and Eng. Sci.)*, 370(12):3359–3384, 2012.
5. Edwin J. Beggs, José Félix Costa, Diogo Poças, and John V. Tucker. An analogue-digital Church-Turing thesis. *Int. Journal of Foundations of Computer Science*, 25(4):373–390, 2014.
6. Emil Post. Degrees of recursive unsolvability. *Bull. of the American Math. Society*, 54, 1948, 641–642.
7. Alan Turing. Systems of logic based on ordinals. *Proceedings of the London Mathematical Society*, Second series, 45:161–228, 1939

Independence Results in Automata Theory

Olivier Finkel

Equipe de Logique Mathématique
Institut de Mathématiques de Jussieu - Paris Rive Gauche
CNRS et Université Paris 7, France.
Olivier.Finkel@math.univ-paris-diderot.fr

Keywords: Automata and formal languages; logic in computer science; infinite words; finite words; 1-counter Büchi automaton; 2-tape Büchi automaton; timed automaton; context-free grammars; pushdown automaton; 2-tape automaton; models of set theory; Incompleteness Theorems; large cardinals; inaccessible cardinals; independence from the axiomatic system "**ZFC** + there exist n inaccessible cardinals".

We prove many independence results in Automata Theory, showing that Incompleteness is a very general phenomenon for automata over infinite words, and even for automata over finite words.

For instance, we proved in [Fin15] that there exist some 1-counter Büchi automata $\mathcal{A}_n$ for which some elementary properties are independent from strong set theories like $T_n =:$ **ZFC** + "There exist (at least) n inaccessible cardinals", for integers $n \geq 1$. We first prove that "$L(\mathcal{A}_n)$ is Borel", "$L(\mathcal{A}_n)$ is arithmetical", "$L(\mathcal{A}_n)$ is ω-regular", "$L(\mathcal{A}_n)$ is deterministic", and "$L(\mathcal{A}_n)$ is unambiguous" are equivalent to the consistency of the theory T_n. This implies that, if T_n is consistent, all these statements are provable from **ZFC** + "There exist (at least) $n + 1$ inaccessible cardinals" but not from **ZFC** + "There exist (at least) n inaccessible cardinals". Notice that the same results can be proved for other large cardinals like hyperinaccessible or Mahlo cardinals.

References

[Fin09] O. Finkel. The complexity of infinite computations in models of set theory. *Logical Methods in Computer Science*, 5(4:4):1–19, 2009.

[Fin11] O. Finkel. Some problems in automata theory which depend on the models of set theory. *RAIRO - Theoretical Informatics and Applications*, 45(4):383–397, 2011.

[Fin15] O. Finkel. Incompleteness theorems, large cardinals, and automata over infinite words. In Magnús M. Halldórsson, Kazuo Iwama, Naoki Kobayashi, and Bettina Speckmann, editors, *Automata, Languages, and Programming - 42nd International Colloquium, ICALP 2015, Kyoto, Japan, July 6-10, 2015, Proceedings, Part II*, volume 9135 of *Lecture Notes in Computer Science*, pages 222–233. Springer, 2015.

[HMU01] J. E. Hopcroft, R. Motwani, and J. D. Ullman. *Introduction to automata theory, languages, and computation.* Addison-Wesley Publishing Co., Reading, Mass., 2001. Addison-Wesley Series in Computer Science.

[Jec02] T. Jech. *Set theory, third edition.* Springer, 2002.

One-point Extensions of Uniformly and Conditionally Computable Real Functions

Ivan Georgiev

Prof. Assen Zlatarov University,
Faculty of Natural Sciences,
Prof. Yakimov Str. 1, 8010, Burgas, Bulgaria,
ivandg@yahoo.com

We consider two notions for relative computability of real functions. The first notion is uniform computability, which is a relativized version of a notion of Grzegorczyk from [1]. The second notion is conditional computability, which extends the uniform computability by allowing the approximation process to depend on an additional natural parameter. The elementary functions of calculus turn out to be conditionally computable with respect to a small subrecursive class of operators and also uniformly computable with respect to the same class of operators, when restricted to compact subsets of their domains. The aim of this talk is to show that under some natural assumptions, the uniform computability is preserved after one-point extensions. We also show by a counterexample that a similar result for the conditional computability does not hold.

Keywords: uniformly computable real functions, conditionally computable real functions, subrecursive classes, one-point extension

References

1. Grzegorczyk, A., Computable functionals. Fund. Math., vol. 42, 168–202 (1955)
2. Skordev, D., Georgiev, I., On a relative computability notion for real functions. CIE Proceedings, Lecture Notes in Computer Science, vol. 6735, 270–279 (2011)
3. Skordev, D., Weiermann, A., Georgiev, I., $\mathcal{M}^2$-computable real numbers. Journal of Logic and Computation, vol. 22 (issue 4), 899–925 (2012)

A Nondeterministic Model for Abstract Geometrical Computation

Rakhshan Harifi and Sama Goliaei

University of Tehran, Tehran, Iran
{rakhshan.harifi,sgoliaei}@ut.ac.ir

A signal machine is an abstract geometrical model for computation, proposed as an extension to the one-dimensional cellular automata, in which discrete time and space of cellular automata is replaced with continuous time and space in signal machine. A signal machine is defined as a set of meta-signals and a set of rules. Computation in a signal machine starts from an initial configuration which is a set of signals and their initial positions. Signals are moving in space freely until a collision occurs. Rules of signal machine specify what happens after a collision, or in other words, specify out-coming signals for each set of colliding signals. Originally signal machine is defined by it's deterministic rules as a deterministic machine.

In this paper, we introduce the concept of non-deterministic signal machine, which may contain more than one defined rule for a set of colliding signals. We define k-restricted nondeterministic signal machine (k-*RNSM*) as a nondeterministic signal machine which has at most two defined rules for each collision and accepts an input if an accept signal is produced in at most k collisions. We show that for each k-*RNSM*, there is an equivalent deterministic signal machine computing the same result, for any given initial configuration.

The idea of the proof is to produce all possible paths of nondeterministic computations in k-*RNSM* on the top of the fractal cloud [2], and test if one of them leads to an accept signal or not. Since for each k-*RNSM* there are at most k collisions before production of accept signal, and there are at most two alternative rules for each collision point, we have to check at most 2^k paths of computation. First we produce 2^k k-bit binary numbers using a beam of k signals and combinatorial comb structure [1], and generate a copy of the initial configuration in each branch of the comb. Then, we follow computation in each branch of the comb according to the corresponding binary number, where each bit of the binary number specifies the applicable rule in the corresponding collision.

References

1. Duchier, D., Durand-Lose, J., Senot, M.: Fractal parallelism: Solving sat in bounded space and time. In: Algorithms and Computation, pp. 279–290. Springer (2010)
2. Duchier, D., Durand-Lose, J., Senot, M.: Computing in the fractal cloud: modular generic solvers for sat and q-sat variants. In: Theory and Applications of Models of Computation, pp. 435–447. Springer (2012)

Borel Functors and Interpretations

Matthew Harrison-Trainor[1], Russell Miller[2], and Antonio Montalbán[1]

[1] University of California, Berkeley
Berkeley, CA, 94720, USA
[2] Queens College, City University of New York
Flushing, NY, 11367, USA
matthew.h-t@berkeley.edu

Given an interpretation of a structure A in a structure B, we get a functor from copies of B to copies of A. If the interpretation uses only computable Σ^0_1 formulas, then the functor will be computable; in general, the functor will be Borel. We show that there is actually a correspondence between functors and interpretations: each Borel functor arises from an interpretation (which may use infinitary formulas).

Similarly, an interpretation of A in B induces a continuous homomorphism from the automorphism group of B to that of A. The reversal is also true.

Keywords: computable structure theory, Borel functors, interpretations

Homomorphic Encryption Schemes

Kelsey Horan

The Graduate Center, CUNY

In this talk I will present two methods of obtaining a Fully Homomorphic Encryption scheme. These methods deviate from the prior known bootstrapping method given by C Gentry in "Fully homomorphic encryption using ideal lattices." These schemes are relatively computationally efficient and conceptually simpler than previous schemes and rely on the General Learning with Errors assumption for security. The talk is based on a work by Z Brakerski, C Gentry, V Vaikuntanathan, "(Leveled) fully homomorphic encryption without bootstrapping" as well as another work by C Gentry, A Sahai, B Waters, "Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based".

An Intuitionistic Formula Hierarchy Based on High-School Identities

Danko Ilik and Taus Brock-Nannestad

Inria & LIX, Ecole Polytechnique
91128 Palaiseau Cedex, France

We revisit intuitionistic proof theory from the point of view of the formula isomorphisms arising from high-school identities.

We first show how any sequent calculus for intuitionistic proposition logic, and in particular the G4ip calculus of Vorob'ev, Hudelmaier, and Dyckhoff, can be represented as a complete proof calculus that nevertheless contains no invertible proof rules, called their high-school (HS) variant.

We then show that all the rules of G4ip and HS admit an arithmetical interpretation, namely each such proof rule can be reduced to an inequality between exponential polynomials.

Finally, we extend the exponential polynomial analogy to the first-order quantifiers, showing that it gives rise to a simple intuitionistic hierarchy of formulas, the first one that classifies formulas up to isomorphism, and proceeds along the same equivalences that lead to the classical arithmetical hierarchy.

References

1. Brock-Nannestad, T., Ilik, D.: An intuitionistic formula hierarchy based on high-school identities. arXiv:1601.04876 (2016)

Subrecursive Sum Approximations of Irrational Numbers

Lars Kristiansen[1,2]

[1] Department of Mathematics, University of Oslo, Norway
[2] Department of Informatics, University of Oslo, Norway

We consider various ways to represent irrational numbers by subrecursive functions: via Cauchy sequences, Dedekind cuts, trace functions, several variants of sum approximations and continued fractions. Let $\mathcal{S}$ be a class of subrecursive functions. The set of irrational numbers that can be obtained with functions from $\mathcal{S}$ depends on the representation. We compare the sets obtained by the different representations. In this talk we will focus on sum approximations.

A function $C : \mathbb{N} \to \mathbb{Q}$ is a *Cauchy sequence* for the real number α when $|\alpha - C(n)| < 1/2^n$. A function $D : \mathbb{Q} \to \{0, 1\}$ is a *Dedekind cut* of the real number α when $D(q) = 0$ iff $q < \alpha$. A function $T : \mathbb{Q} \to \mathbb{Q}$ is a *trace function* for the irrational number α when $|\alpha - q| > |\alpha - T(q)|$. An irrational number α can also be represented by a function $f : \mathbb{N} \to \mathbb{Z}$ where $f(n)$ yields the n^{th} element of the continued fraction $[a_0; a_1, a_2 \ldots]$ of α.

Any irrational number α can be written of the form $\alpha = a + \frac{1}{2^{k_0}} + \frac{1}{2^{k_1}} + \frac{1}{2^{k_2}} + \ldots$ where $k_0, k_1, k_2, \ldots$ is a strictly monotone increasing sequence of natural numbers and a is an integer. Let $A : \mathbb{N} \to \mathbb{N}$ be a strictly monotone function. We will say that A is a *sum approximation from below* of the the real number α if there exists $a \in \mathbb{Z}$ such that $\alpha = a + \sum_{i=0}^{\infty} 1/2^{A(i)+1}$. Any real number can also be written as a difference between an integer and an infinite sum, and we will say that A is a *sum approximation from above* of the the real number α if there exists $a \in \mathbb{Z}$ such that $\alpha = a - \sum_{i=0}^{\infty} 1/2^{A(i)+1}$.

The sum approximations defined above are sum approximations in base 2. We will also consider *general sum approximations* (from above and below). A *general sum approximations* of α is a function that yields the sum approximation of α in any base.

Let $\mathcal{P}_C$, $\mathcal{P}_D$ and $\mathcal{P}_{[]}$ denote the sets of irrationals that are representable, receptively, by primitive recursive Cauchy sequences, primitive recursive Dedekind cuts and primitive recursive continued fractions. Specker [3] proved $\mathcal{P}_D \subset \mathcal{P}_C$, and Lehman [2] proved $\mathcal{P}_{[]} \subset \mathcal{P}_D$ (strict inclusions). Let $\mathcal{P}_T$ denote the sets of irrationals that are representable by primitive recursive Trace functions. It is proved in [1] that $\mathcal{P}_T = \mathcal{P}_{[]}$. We will present some theorems on how (general) sum approximation (from above and below) relate to the other representations. These theorems are extensions and refinements of theorems found in [1].

References

1. L. Kristiansen, *On subrecursive representability of irrational numbers.* Accepted for publication in Computability (the journal of CiE).
2. R. S. Lehman, On Primitive Recursive Real Numbers, *Fundamenta Mathematica* **49**(2) (1961), 105–118.
3. E. Specker, Nicht Konstruktiv Beweisbare Satze Der Analysis, *The Journal of Symbolic Logic* **14**(3) (1949), 145–158.

Connecting Weihrauch reducibility and intuitionistic reverse mathematics

Rutger Kuyper

Victoria University of Wellington, New Zealand
mail@rutgerkuyper.com
WWW home page: http://rutgerkuyper.com

In this talk we will present a contribution to the recent interest in the intuitive similarity between reverse mathematics and Weihrauch reducibility. There are currently two main approaches to formalising this connection. The first of these proceeds by formalising Weihrauch reducibility within reverse mathematics, an approach which was pioneered by Dorais et al. and Dzhafarov.

The other approach is to connect Weihrauch reducibility to intuitionistic reverse mathematics, building on the long-standing intuition that there is a tight connection between intuitionistic logic and computability. One of the fields studying this connection goes under the name of realisability. Techniques from realisability have first been brought into the setting of reverse mathematics by Hirst and Mummert, whose work was continued by Dorais, and by Fujiwara, in their work on the reverse mathematical strength of sequential versions of theorems.

We present a precise connection between Weihrauch reducibility and provability in intuitionistic reverse mathematics, building on the work of the authors mentioned in the previous paragraph. Roughly speaking, we show that a Π^1_2-statement α implies a second Π^1_2-statement β over EL_0, the intuitionistic version of RCA_0, plus Markov's principle, if and only if β Weihrauch-reduces to α. Of course, one quickly realises the theorem cannot be true as stated, but we give a precise way to state the theorem using the notion of composition in the Weihrauch degrees, and we also show that the statement just given holds if we restrict our intuitionistic calculus to an affine variant (i.e. a version which excludes some of the contraction rules in its sequent calculus).

When error-correcting codes meet computability theory

Benoit Monin

Université Paris-Est Créteil

Generic-case complexity is a subfield of computational complexity. It started with the observation that some problems that are difficult to solve in full are easy to solve on "most inputs", namely on a set of inputs of asymptotic lower density 1. This notion was introduced by Kapovich, Myasnikov, Schupp and Shpilrain. They showed among other things that for a large class of finitely generated groups, the generic case complexity of the word problem is linear.

This notion has recently been extended by Jockusch and Schupp. The authors identified two notions that can be proved to be incomparable. The first is generic computability, where one must always give the right answer, without having to provide an answer for a small set of input. The second is coarse computability, for which one always have to provide an answer, with the right of being wrong on a small set of inputs. In both cases, a set of inputs is considered small if it is of asymptotic upper density 0.

Then Andrews, Cai, Diamondstone, Jockusch and Lempp assigned in "Asymptotic density, computable traceability and 1-randomness" a value gamma (with lower case 'g') to each set of natural numbers, which indicates how far the set is from being coarse-computable. They used this to assign a value Gamma (with upper case 'G') to each Turing degree, which indicates how far the degree is from being coarse-computable. They proved that the Gamma values of 0, 1/2 and 1 can be realized. They also proved that if a Turing degree has a Gamma value strictly larger than 1/2, then it is the computable degree and its Gamma value in fact equals 1. They asked whether a Turing degree can have a Gamma value strictly in between 0 and 1/2.

Using notions from computability theory, developped by Monin and Nies, together with some techniques from the field of error-correcting codes, we are able to give a negative answer to this question: The only Gamma values that can be realized by a Turing degrees are $0, 1/2$ and 1.

Natural Language Semantics and Computability

Richard Moot[1] and Christian Retoré[2]

[1] CNRS LaBRI
[2] Université de Montpellier & LIRMM

We present an overview of known results about the computability of natural language semantics. We do no discuss new models or new results in the formal semantics of natural language, but rather analyse, from the point of view of computability and computational complexity, the logical models and algorithms currently used in natural language semantics.

We are interested, following [1], in formal semantics as a mapping from a natural language sentence to a (set of) logical formulas corresponding to its meanings (there can be multiple formulas because a natural language statement can be ambiguous). Such computational systems of formal semantics are useful as components for many tasks requiring natural language understanding, such as question-answering and automated translation. We argue that as long as possible world semantics is left out, one can compute the semantic representation(s) of a given statement, including aspects of lexical meaning. We also discuss the known results about the algorithmic complexity of the processes involved. In the context of categorial grammar in the logical tradition — such as the Lambek calculus and related systems — this involves studying 1) the complexity of parsing/theorem proving for such systems and 2) the complexity of computing the meaning given such a parse/proof. More details can be found in the report [2].

References

1. Montague, R.: The proper treatment of quantification in ordinary English. In Thomason, R., ed.: Formal Philosophy. Selected Papers of Richard Montague. Yale University Press (1974)
2. Moot, R., Retoré, C.: Natural language semantics and computability. Technical report, LaBRI and LIRMM (2016) `https://hal.inria.fr/hal-01315316`.
3. Moot, R., Retoré, C.: The Logic of Categorial Grammars: A Deductive Account of Natural Language Syntax and Semantics. Springer (2012)

Gaps distribution in the infinite time Turing machines clockable ordinals

Sabrina Ouazzani

LIRMM CNRS, Université de Montpellier

Infinite time Turing machines (ITTM) are a computational model introduced in 2000 by Hamkins and Lewis in [HL00]. This model generalises the computation process of Turing machines to ordinal time: computation steps are indexed by ordinals. Configurations at successor steps are obtained in the classical way, while configurations at limit steps are obtained by specific operations (namely a lim sup on the cells and a rewind of the head which is put in a special lim state).

ITTM work on infinite binary strings. We can encode a countable ordinal on an infinite binary string by encoding a well-founded order of same order type on $\mathbb{N}$. Therefore, inputs and outputs of ITTM can be (countable) ordinals.

Two notions appear naturally. An ordinal α is *clockable* if there exists an ITTM which halts on input "$000\ldots$" in α steps of computation. It is *writable* if there exists an ITTM which outputs a code for α on input "$000\ldots$" and halts. Welch has shown in [Wel09] that these two kinds of ordinals have the same supremum, called λ, which is a countable ordinal.

All ordinals below λ are writable. But there exist times at which no ITTM halt. Indeed, Hamkins and Lewis have shown in [HL00] that there are gaps in the clockable ordinals. The begining and the end of these gaps are limit ordinals. The goal of this work is to give a more precise description of their size distribution.

Welch proved that gaps begin by admissible ordinals. Moreover, λ can be caracterised in terms of admissibiliy [HL00]. In the same paper, the authors also proved that there are gaps of arbitrary large sizes. Another important result of the litterature is that the size of the first gap above any clockable ordinal is ω.

In this talk, we prove the existence of gaps with specific properties. In particular, we prove that for all *writable* limit ordinal α, there exist gaps of size *exactly* α (*i.e.* there are gaps of all "possible" size). We also prove that there exists an ordinal β such that β starts a gap of size β. We explicitely provide the ITTM algorithms which prove the existence of such gaps.

This is a joint work with Bruno Durand and Gregory Lafitte.

References

[HL00] Joel D. Hamkins and Andrew Lewis. Infinite time turing machines. *Journal of Symbolic Logic*, 65(2):567–604, 2000.

[Wel09] Philip D. Welch. Characteristics of discrete transfinite time turing machine models: Halting times, stabilization times, and normal form theorems. *Theoretical Computer Science*, 410(4-5):426–442, 2009.

Computational Complexity for Ordinal Turing Machines

Benedikt Löwe[1,2] and Benjamin Rin[1]

[1] Institute for Logic, Language, and Computation, Universiteit van Amsterdam, Postbus 94242, 1090 GE Amsterdam, The Netherlands, {b.loewe,b.g.rin}@uva.nl
[2] Fachbereich Mathematik, Universität Hamburg, Bundesstraße 55, 20146 Hamburg, Germany

In our talk, we shall explore the subject of computational complexity theory within the generalized setting of transfinite computability.

Previously, work in this area has focused on the infinite time Turing machine (ITTM) model of Hamkins and Lewis, which generalizes Turing machines to allow for transfinite computational run time. E.g., Schindler (2003) proved that $\mathbf{P} \neq \mathbf{NP}$ for such machines (a result later strengthened by Deolalikar, Hamkins, and Welch, 2005, to $\mathbf{P} \subsetneq \mathbf{NP} \cap \mathbf{co\text{-}NP}$). However, in finitary complexity theory, the time used by a computation, the length of the input, and the space used by a machine are natural numbers, i.e., measured on a comparable scale. This breaks down for ITTMs since the tape length is ω, but the computations in general take a transfinite amount of time. Löwe (2006) and Winter (2007, 2009) defined notions of space complexity for ITTMs in terms of the complexity rather than the length of the input.

The symmetry between time and space is restored in Koepke's Ordinal Turing Machines (OTMs) which have both ordinal-length time and space. In this talk, we define notions of $\mathbf{P}$, $\mathbf{NP}$, $\mathbf{PSPACE}$, and other complexity classes for OTMs, generalizing some definitions due to Winter (2007, 2009).

Thus we can say, e.g., that an OTM runs in *polynomial time* if there is an ordinal β such that for every input of length ν, the machine halts in fewer than ν^β steps (where ν^β denotes ordinal exponentiation). Based on this, we define the class of *polynomial time decision problems* as those that are decided by a polynomial time OTM, and likewise for OTM analogues of $\mathbf{NP}$, polynomial space, exponential time and space, and other complexity classes.

We can now formulate ordinal versions of problems such as CLIQUE, SUBSET-SUM, TRAVELING SALESMAN, SAT, 3-SAT, and so on, and explore their properties with respect to the mentioned OTM complexity classes. Naturally, we may then consider whether classical results such the Cook-Levin theorem, the Baker-Gill-Solovay theorem, Ladner's theorem, and others generalize to the transfinite setting. This talk will present definitions and initial results.

Complexity of Relations via Computable Reducibility

Luca San Mauro

Vienna University of Technology

Computable reducibility provides a natural way of ranking binary relations on ω according to their complexity. Such reducibility is defined as follows: let R and S be two binary relations, we say that R is *computably reducible* to S iff there is a computable function f such that, for all $x, y \in \omega$, the following holds:

$$xRy \Leftrightarrow f(x)Sf(y).$$

Computable reducibility has been object of study for decades, being mostly applied to the case of equivalence relations. In particular, a prominent problem in the area has been that of characterizing universal equivalence relations, i.e. relations to which all others relations, of a given complexity, can be computably reduced.

In this talk, we address the problem of universality for a more general context than that of equivalence relations. First, we prove that, contrary to the case of equivalence relations and preorders, for each level of the arithmetical hierarchy there is a universal binary relation. Then, we define natural examples of universal Σ^0_n binary relations and of universal Π^0_n binary relations, obtained by fairly simple manipolations of the two most fundamental set-theoretic relations. More precisely, let $U^{\in}_n$ be the following Σ^0_n binary relation,

$$xU^{\in}_n y \Leftrightarrow x \in W_y^{\emptyset^{(n-1)}},$$

and, for $n > 2$, let $U^{\subseteq}_n$ be the following binary relation

$$xU^{\subseteq}_n y \Leftrightarrow W_x \subseteq W_y^{(n-2)}.$$

. We show that:

1. For all n, $U^{\in}_n$ is a universal Σ^0_n binary relation;
2. For $n > 2$, $U^{\subseteq}_n$ is a universal Π^0_n binary relation.

References

1. Uri Andrews, Steffen Lempp, Joseph S. Miller, Keng Meng Ng, Luca San Mauro, Andrea Sorbi, *Universal computably enumerable equivalence relations*, ***The Journal of Symbolic Logic***, vol. 79 (2014), no. 1, pp. 60–88.
2. Egor Ianovski, Russell Miller, Keng Meng Ng, André Nies, *Complexity of equivalence relations and preorders from computability theory*, ***The Journal of Symbolic Logic***, vol. 79 (2015), no. 3, pp. 859–881.
3. Luca San Mauro, *Infomal Proofs and Computability*, **PhD Thesis**, SNS, Pisa (2015).

Is the Inverse Problem for Iterated Function Systems Undecidable?

Anargyros Sarafopoulos

National Centre for Computer Animation,
Bournemouth University,
Talbot Campus, Fern Barrow, Poole UK
{asarafop}@bournemouth.ac.uk

Abstract. Iterated Function Systems (IFS) [1] provide a well known mathematical framework for studying a wide variety of fractal structures. Here we focus on the inverse problem for IFS. We suggest that in general optimal solutions for the inverse problem for IFS are not feasible.

Keywords: IFS Fractals, Computability Theory, Computable Analysis

1 Introduction

Iterated function systems (IFS) have been studied extensively and have many applications in image and signal compression as well as computer graphics; see for example Barnsley's textbook [1]. Nevertheless the IFS inverse problem (as stated originally by Barnsley in [1]) remains open; there is no known algorithm to solve the inverse IFS problem optimally or decide whether exact solutions exists.

We define the optimal inverse IFS problem using notation and ideas from Computable Analysis [2]. It is worth noting that an optimal IFS I in this context is very different from the optimal encoding of IFS I using a Turing Machine (TM) or other equivalent computer programs or functions. This is because IFS are not equivalent to computer programs; an IFS can't simulate a Turing Machine (TM). The problem of minimum length IFS codes is therefore different to the general minimum description length problem of equivalent TMs which is known to be undecidable.

Although IFS are not computer programs we still believe that the optimal inverse problem for IFS can be shown to be undicatable using a reduction to the halting problem or the equivalent notion of the halting problem in Computable Analysis, which is; non continuous functions are not computable, or there is no computable function which can compare two real values for equality.

References

1. M. F. Barnsley. *Fractals Everywhere.* Academic Press, London, 1988.
2. K. Weihrauch. *Computable Analysis: An Introduction.* Texts in Theoretical Computer Science. An EATCS Series. Springer, 2000.

Honest elementary degrees without the cupping property

Paul Shafer

Department of Mathematics, Ghent University, Krijgslaan 281 S22, B-9000 Ghent, Belgium

An element a of a lattice *cups* to an element $b > a$ if there is a $c < b$ such that $a \cup c = b$. An element of a lattice has the *cupping property* if it cups to every element above it. We study cupping in the lattice of *honest elementary degrees*, in which functions with elementary recursive graphs are compared via the 'elementary recursive in' relation. Kristiansen [2] showed that every sufficiently large honest elementary degree has the cupping property. This result prompted Kristiansen, Schlage-Puchta, and Weiermann [3] to ask if every non-zero honest elementary degree has the cupping property. We answer their question negatively by showing that if $\mathbf{b}$ is a sufficiently large honest elementary degree, then there is a non-zero honest elementary degree $\mathbf{a} <_{\mathrm{E}} \mathbf{b}$ that does not cup to $\mathbf{b}$. We also compare cupping in the honest elementary degrees to recent work of Cai [1] on cupping in the *degrees of relative provability*.

References

1. Cai, M.: Higher unprovability (2015), preprint
2. Kristiansen, L.: Subrecursive degrees and fragments of Peano arithmetic. Archive for Mathematical Logic 40(5), 365–397 (2001)
3. Kristiansen, L., Schlage-Puchta, J.C., Weiermann, A.: Streamlined subrecursive degree theory. Annals of Pure and Applied Logic 163(6), 698–716 (2012)

Comparing Notions of Effective Genericity

Rose Weisshaar

University of Notre Dame

In recent work, Cholak, Dzhafarov, Hirst and Slaman showed that for $n \geq 3$, every Mathias n-generic computes a Cohen n-generic. It is natural to wonder how other types of generic objects compare to one another. We consider generics for an effective version of a notion of forcing introduced by Slaman and Groszek in their proof that every set with a modulus has a uniform modulus. We call these generics domination generics (or D-generics). Adapting a method developed by Cholak, Dzhafarov, and Soskova, we show that for $n \geq 3$, every Mathias n-generic computes a D-n-generic, and every D-n-generic computes a Mathias n-generic. Finally, we explore the (open) question of whether, for $n \geq 3$, the Mathias n-generics and the D-n-generics occupy exactly the same Turing degrees.

Rational Grading and Transitivity in Description Logics

Mitko Yanchev e-mail: yanchev@fmi.uni-sofia.bg

Faculty of Mathematics and Informatics, Sofia University 'St. Kliment Ohridski'
5 James Bourchier blvd., 1164 Sofia, Bulgaria

Counting (or *grading* with natural numbers) has been naturally extended to grading with rationals (and even with real coefficients) to enrich the expressive power of modal and description languages. We consider several different approaches known for realizing rational grading, and compare them in their expressivity and reasoning complexity. We focus on the rational grading realized independently from counting through the *modal operators for rational grading* and their analogues in Description Logics (DLs)—the concept constructors, called *part restrictions* [2], both capable of distinguishing a rational part of a set of successors. The presence of separate rational grading constructors in DLs proved beneficial. Together with the use of *indices technique* [2], designed for exploring the rational grading, they allow following a common way for obtaining decidability and complexity results as in less, so in more expressive languages with rational grading.

Next we look at the ways of embedding the notion of transitivity in DLs. These logics are widely used in knowledge-based systems, and the presence of *transitive roles* in a description language permits complex objects to be described by referring to their components without specifying a particular level of decomposition. *Role hierarchies* bring additional expressive power. In DL $\mathcal{ALCQIH}_{R^+}$ [1], with both transitive roles and role hierarchies, the syntax is enriched also with inverse roles and the counting *qualifying number restrictions*. It is given a sound and complete decision procedure for that logic.

Now we consider DL $\mathcal{ALCQPIH}_{R^+}$, an extension of $\mathcal{ALCQIH}_{R^+}$ with part restrictions, where the transitive roles are allowed only outside the qualifying number restrictions and part restrictions. We use the tableaux technique with pair-wise blocking combined with indices technique to prove that the reasoning in the extended logic is decidable. Disallowing the role hierarchies, what usually results in relaxing the reasoning complexity (with the trade-off in expressivity of the language), we obtain DL $\mathcal{ALCQPI}_{R^+}$, having only independent (transitive and non-transitive) roles. We give a PSPACE decision procedure for that logic.

References

1. I. Horrocks, U. Sattler, and S. Tobies. A description logic with transitive and converse roles, role hierarchies and qualifying number restrictions. LTCS-Report 99-08, LuFg Theoretical Computer Science, RWTH Aachen, Germany, 1999.
2. M. Yanchev. A description logic with part restrictions: PSPACE-complete expressiveness. In A. Beckmann, E. Csuhaj-Varjú, and K. Meer, editors, *Collection of Unpublished Abstracts*, CiE 2014, pages 261–270, Budapest, Hungary, 2014.

Author Index